

a

PATENT

Docket No. IL-10360

Assistant Commissioner for Patents
Washington, DC 20231

NEW APPLICATION TRANSMITTAL

Transmitted herewith for filing is the patent application of Inventor(s):
Douglas R. Coffland

For (title): **SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION**

1. Type of Application

- ☒ This new application is for an original patent.
- ☐ This new application is a:
 - ☐ Division
 - ☐ Continuation
 - ☐ Continuation-in-part (CIP)

2. Benefit of Prior U.S. Application(s) (35 USC 120)

- ☐ The new application being transmitted claims the benefit of prior U.S. application(s).

3. ☐ Benefit under 35 U.S.C. 119(e) of United States provisional application(s) listed below:

Application Serial No.	Filing Date
------------------------	-------------

4. Papers enclosed which are required for filing Date Under 37 CFR 1.53(b).

- 13 Pages of specification
- 7 Pages of claims
- 1 Pages of abstract
- 5 Sheets of drawings
 - ☒ formal
 - ☐ informal

5. Additional papers enclosed

- ☐ Preliminary Amendment
- ☒ Information Disclosure Statement
- ☒ Form PTO-1449
- ☐ Special Comments

jc534 U.S. PTO
09/24/99

jc534 U.S. PTO
09/24/99

6. Declaration or oath

- ☒ Enclosed and executed by
- ☒ inventors
 - ☐ legal representative of inventor(s) 37 CFR 1.42 or 1.43
- ☐ Not Enclosed

7. Assignment

- ☒ An assignment of the invention to The Regents of the University of California.
- ☒ is attached
 - ☐ will follow

8. Certified Copy

Certified copy(ies) of application(s)

(country)	(application no.)	(filed)
(country)	(application no.)	(filed)

from which priority is claimed

- ☐ is(are) attached.
- ☐ will follow

9. Fee Calculation

CLAIMS AS FILED					
Type of Claim	Number Filed	Included in Basic Fee	Number Extra	Rate	Total Fee
Total Claims	30	-20 =	10 x	\$18 =	\$ 180.00
Independent Claims	4	-3 =	1 x	\$78 =	\$ 78.00
Multiple Claims				=	\$
Basic Filing Fee				=	\$ 760.00
Sub-Total				=	\$ 1,018.00
Small Entity Filing Fee				=	\$ 509.00

10. Small Entity Statement(s)

- ☒ Verified Statement that this is a filing by small entity under 37 CFR 1.9 and 1.27 is attached.

Filing Fee Calculation (50% of regular filing fee) \$ 509.00

11. Fee Payment

- ☐ Not Enclosed
☒ Enclosed (See Account No. Below)

Total Basic Filing Fees To Be Paid \$ 509.00

12. Method of Payment of Fees

- ☐ Check in the Amount of \$ _____
☒ Charge Account No. 12-0695 in the amount of \$ 509.00

A duplicate of this transmittal is attached.

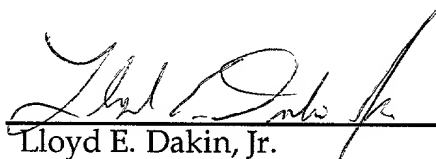
13. Instructions As To Overpayment/Underpayment

- ☒ credit/charge
Account No. 12-0695
☐ refund

Reg. No.: 38,423

Tel. No.: (925) 423-8554

Dated: September 1, 1999


Lloyd E. Dakin, Jr.

P.O. Box 808, L-703
Livermore, CA 94551

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Douglas R. Coffland

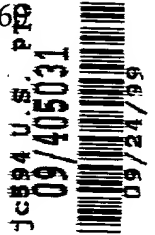
Attorney Docket No. : IL-10369

Serial No. :

Art Unit:

Filed :

Examiner:

For : System and Method for
Multimedia EncryptionAssistant Commissioner for Patents
Washington, D.C. 20231EXPRESS MAIL CERTIFICATE"Express Mail" label number EL269945990USDate of Deposit September 24, 1999I hereby certify that the following *attached*

1. Recordation Cover Sheet
2. Assignment (1 page)
3. New Application Transmittal (in duplicate)
4. Combined Declaration and Power of Attorney (2 pages)
5. Verified Statement Claiming Small Entity Status
6. Application
(Specification 13 pages, Claims 7 pages, Abstract 1 page)
Five (5) sheets of formal drawings;
7. Information Disclosure Statement, Form 1449,
1 copy each of 5 patents and 1 publication
8. Return postcard

is being deposited with the United States Postal Service "Express Mail Post Office to addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box: Patent Application, Washington, D.C. 20231.

Nancy J. Stone

(Type or print name of person mailing paper)

(Signature of person mailing paper or fee)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Douglas R. Coffland Docket No. : IL-10360
 Serial No. : Art Unit :
 Filed : Batch No. :
 For : System and Method for Examiner :
 Multimedia Encryption

**VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY
 STATUS [37 CFR 1.9 (f) and 1.27(d)] - NONPROFIT ORGANIZATION**

I hereby declare that I am an official empowered to act on behalf of the nonprofit organization identified below:

The Regents of the University of California
 1111 Franklin Street
 Oakland, CA 94607-5200

TYPE OF ORGANIZATION

 X University or Other Institution of Higher Education

I hereby declare that the nonprofit organization identified above qualifies as a nonprofit organization as defined in 37 CFR 1.9(e) for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code with regard to the invention entitled System and Method for Multimedia Encryption

by inventor(s) Douglas R. Coffland

described in

 X the specification filed herewith.

 application serial no. _____, filed _____.

 patent no. _____, issued _____.

I hereby declare that rights under contract or law have been conveyed to and remain with the nonprofit organization with regard to the above identified invention, except for a license to a Federal Agency pursuant to 35 USC 202(c) (4).

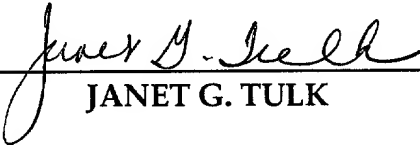
Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

 X no such person, concern, or organization

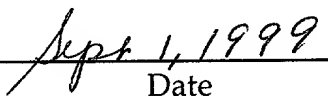
I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true: and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

JANET G. TULK
Laboratory Counsel
Lawrence Livermore National Laboratory
7000 East Avenue, L-701
Livermore, CA 94551



JANET G. TULK



Date

S- 91,131

IL-10,360

SYSTEM AND METHOD FOR
MULTIMEDIA ENCRYPTION

BY

Douglas R. Coffland (USA)
5674 Wisteria Way
Livermore, CA 94550

1 SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION

2

3 The United States Government has rights in this invention pursuant
4 to Contract No. W-7405-ENG-48 between the United States Department of
5 Energy and the University of California for the operation of Lawrence
6 Livermore National Laboratory.

7

8 BACKGROUND OF THE INVENTION

9 1. Field of the Invention

10 The present invention relates generally to systems and methods for
11 encryption, and more particularly for multimedia encryption.

12 2. Discussion of Background Art

13 Transmission of audio and video signals, such as video conferencing
14 and security surveillance signal, across both local and wide area networks is
15 becoming more and more commonplace in today's globally interconnected
16 internet driven economy. In such applications, encryption is often required
17 for protecting and authenticating such multimedia signals as they travel over
18 unsecured networks. For instance, corporations often exchange business
19 sensitive information during such conferences which must not be
20 intercepted. Additionally, multimedia information from networked security
21 camera systems must be authenticated and protected from unauthorized
22 monitoring.

1 A degree to which encryption authenticates and protects multimedia
2 data depends on the encryption schema used, an encryption key length, the
3 predictability of the encryption key, and how the encryption keys are
4 protected. Typically, encryption keys are generated by hashing algorithms
5 from random number seeds provided by a source which hopefully provides
6 random number seeds. Random number seeds, however, are extremely
7 difficult if not impossible to generate using algorithmic methods on digital
8 computers, since algorithms executing on digital computers are by nature
9 deterministic. As a result, various external chaotic sources have been used to
10 generate the random number seeds.

11 Examples include methods described in U.S. Patent 5,732,138 entitled,
12 "Method For Seeding A Pseudorandom Number Generator With A
13 Cryptographic Hash Of A Digitization Of A Chaotic System," by Noll et al.,
14 and U.S. Patent 5,774, 549 entitled, "Method And Apparatus That Processes A
15 Video Signal To Generate A Random Number Generator Seed" by Jakob
16 Nielsen.

17 Noll discusses generating seeds by applying a hashing algorithm to a
18 digitized chaotic system. Chaotic systems mentioned include clouds moving
19 in the sky, ocean waves crashing on a shoreline, and nodules moving within
20 a "lava-lamp." A weakness of the Noll system, however, is that in his
21 preferred embodiment, new seed generation depends upon using dedicated
22 input devices to monitor "real-world scenes," such as a video camera

1 monitoring a lava-lamp, in order to obtain the necessary chaotic input for
2 eventual random number generation.

3 Nielsen also requires dedicated input devices, such as a video camera.

4 Nielsen monitors “live” scenes with a video camera and then generates
5 seeds from pixel changes within sequential frames of video data. A weakness
6 of the Nielsen system is that new seeds are not generated when motion
7 within a monitored scene stops.

8 In response to the concerns discussed above, what is needed is a system
9 and method for multimedia encryption that overcomes the problems of the
10 prior art.

SUMMARY OF THE INVENTION

The present invention is a system and method for multimedia encryption. Within the system of the present invention, a data compression module receives and compresses a media signal into a compressed data stream. A data acquisition module receives and selects a set of data from the compressed data stream. And, a hashing module receives and hashes the set of data into a keyword.

In other aspects of the invention, the system may include a data compression module that compresses the media signal into any compression format that has varying length data frames. Examples of media compression formats that with varying length data frames include MPEG1, MPEG2, MPEG4, MJPEG, and H.261. The set of data can be one frame of data, cross over several frame boundaries, include compression transform coefficients, include predictive data frames. Finally, a pseudo-random number generator can processes a single keyword seed in to a set of keywords.

The method of the present invention includes the steps of compressing a media signal into a compressed data stream; selecting a set of data from the compressed data stream; and hashing the set of data into a keyword.

The system/apparatus and method of the present invention are particularly advantageous over the prior art because a means of capturing random numbers for encryption seeding directly from variable frame boundary compressed data is disclosed. In light of a growing importance in

1 securely transmitting multimedia data over digital networks, obtaining
2 random numbers directly from the multimedia data would be very useful.
3 These and other aspects of the invention will be recognized by those
4 skilled in the art upon review of the detailed description, drawings, and
5 claims set forth below.

BRIEF DESCRIPTION OF THE DRAWINGS

- 1
- 2 Figure 1 is a block diagram of a system for multimedia encryption
- 3 according to the present invention;
- 4 Figure 2 is a graphical depiction of quantization processes within an
- 5 analog-to-digital converter within the system;
- 6 Figure 3 is a block diagram of a computer within the system;
- 7 Figure 4 is a graphical depiction of how a data acquisition module
- 8 operates within the system; and
- 9 Figure 5 is a flowchart of a method for multimedia encryption.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 is a block diagram of a system 100 for multimedia encryption according to the present invention. Within the system 100, a transducer 102, such as a video camera, a radio, a microphone, a Geiger counter, or an electrical component, outputs a media signal 104.

The media signal 104 may or may not contain useful information, such as an actual video scene or audio output, and the present invention does not require that useful information be present. For example, while a video camera could be capturing a scene, this is not required, and instead a lens-cap could be on the camera causing the scene to be perfectly quiescent. In one embodiment of the present invention, the media signal need only include random transducer noise having a noise signal amplitude. Random noise is not the same as chaotic noise. Random noise, such as white Gaussian noise, is completely unpredictable from one moment to a next, while chaotic noise is highly predictable over short time periods. In a second embodiment of the invention, however, random transducer noise need not even be present. Instead, data compression techniques provide a basis for multimedia encryption, as will be elaborated upon below.

The media signal 104 from the transducer 102 is fed into an analog-to-digital (A/D) converter 106. The converter 106 quantizes the media signal with a quantization step size smaller than the noise signal amplitude within the media signal 104, creating a quantized media signal 108. The quantized media signal 108 is then routed to a computer 110.

1

2 Figure 2 is a graphical depiction of quantization processes within the
3 analog-to-digital converter 106 within the system 100. The media signal 104 is
4 periodically sampled 202. The samples 202 are then quantized at predefined
5 steps 204 resulting in the quantized media signal 108. The quantized media
6 signal 108 is a quantized approximation of the media signal 104 containing
7 random transducer noise. The random noise in the media signal 104 will
8 cause even unchanging video scenes to have quantization values 206 which
9 fluctuate for media signal values close to one or more quantization steps 204.
10 Thus, even a perfectly quiescent media signal 104 (e.g. when a lens cap is on a
11 video camera containing the transducer 102) will contain some randomness
12 from random transducer noise. Put another way, as long as a size of a
13 smallest quantizer step is no larger than an amplitude of the transducer 102
14 noise, the quantized media signal 108 will include a high level of randomness
15 even if input to the transducer is perfectly quiescent.

16 Typically, the transducer noise is sufficient to cause the quantization
17 values 206 to fluctuate. However, if the transducer noise is small relative to
18 the quantization steps 204, then either video or audio content of the media
19 signal 104 must vary somewhat so that what little noise is in the scene will
20 enable random noise to be quantized by the A/D converter 106. Randomness
21 will be present in the media signal 104 when an actual sampled media signal
22 value 208 is very close to a quantization boundary 210. When this occurs, a
23 small transducer 102 signal will randomly cause the quantized media signal

1 108 to vary. It is possible to test whether sufficient random noise is present
2 within the media signal 104 by looking at least significant bits of the media
3 signal 104 and ensuring that no long sequences of a single bit value (i.e. ones
4 or zeros) exist. Long sequences of zeros or ones in a least significant bit of the
5 media signal 104 would suggest that the random noise is not of a sufficient
6 amplitude to create random numbers.

7 In an alternate embodiment, distortion may be introduced into the
8 media signal 104 generated by the transducer 102 such that the random
9 transducer noise will have an amplitude greater than the quantization steps
10 204. Distortion may be introduced, for example, in a video camera by turning
11 on an automatic gain control and increasing video camera gain. In another
12 embodiment, focus and zoom of the camera can be varied while capturing
13 video data.

14
15 Figure 3 is a block diagram 300 of the computer 110 within the system
16 100. Within the computer 110, a data compression module 302 compresses the
17 quantized media signal 108 into a compressed data stream 303 using any
18 number of formats, such as MJPEG, MPEG1, MPEG2, MPEG4, or H.261. Many
19 other standard, as well as proprietary, media compression schemes also exist
20 that are compatible with the present invention.

21 The compressed data stream 303 is partitioned into data frames of
22 varying length, depending upon an amount of information contained in the
23 media signal 104, variations in a scene or audio captured by the transducer

1 102, transducer noise, and system noise. For example, a 16384 byte amount of
2 data acquired from an MPEG1 compressed data stream can include between
3 one and eight frames of media data of varied length. For comparison,
4 uncompressed media signals generally have a frame length which is fixed in
5 size. For instance, uncompressed digital video signals include a series of fixed
6 sized digital video images.

7 Under some compression schemas, the compressed data stream 303
8 includes predictive data frames. Predictive data frames only contain
9 information which reports on differences between a current data frame and a
10 most recent full data frame. Predictive data frames typically include motion
11 vectors and error codes. Identical motion vectors and error codes between
12 full frames indicate an absence of any video motion, audio, or transducer
13 noise.

14 The compressed data stream 303 also can include compression
15 transform coefficients, frame sequence numbers, and cyclic redundancy
16 checks which vary from frame to frame. Identical transform coefficients
17 between full frames indicate an absence of any video motion, audio, or
18 transducer noise.

19 In response to a key request 304 received from an external source (not
20 shown), a control module 306 instructs a data acquisition module 308 to
21 collect a set of data 309 from the compressed data stream 303. The data
22 acquisition module 308 operating in conjunction with the data compression
23 module 302 creates a robust source of random numbers in the set of data 309.

1 This is due to unpredictable variability between the compressed data stream
2 303 and random selection of the set of data 309 therefrom.

3 In an alternate embodiment, the data acquisition module 308 can be
4 instructed to collect the set of data 309 directly from the quantized media
5 signal 108 output by the A/D converter 106 before any data compression. An
6 amount of data collected is dependent upon an amount of uncertainty
7 required for a given application. A good rule of thumb is to capture an
8 amount of data greater than or equal to a compressed full frame. However,
9 when a large amount of noise is present in the media signal, a lesser amount
10 of the media signal data needs to be collected.

11 A message digest generator 310 receives and processes the set of data
12 309 with a hashing algorithm. The message digest generator 310 generates a
13 fixed-length unique identifier 311 for each pattern of bits in the set of data 309.
14 Hashing algorithms assure that the resultant identifier 311 varies significantly
15 even if the set of data 309 only varies by one bit. It is computationally
16 infeasible to reconstruct the set of data 309 from only knowledge of the
17 identifier 311. This identifier 311 is also called a keyword seed.

18 An encryption key generator 312 is a pseudo-random number
19 generator that receives and processes the identifier 311 into a set of keywords
20 to be immediately used or stored in a memory 314 for later use.

21

22 Figure 4 is a graphical depiction 400 of how the data acquisition module
23 308 operates within the system 100. Shown is a typical compressed

1 multimedia data stream 402. The data stream 402 includes compressed audio,
2 video, and control data separated by frame boundaries 404. Each frame of data
3 has a length, such as video data 406, which has a length 408. Within the
4 multimedia data stream, lengths of each frame vary randomly, depending on
5 a compression ratio as well as other well known compression algorithm
6 factors. The data acquisition module 308 acquires a set of data 410 from the
7 compressed data stream 303 without regard to any of these factors.

8 Thus, the set of data 410 can cross over the frame boundaries 404 in a
9 random manner, resulting in a highly random, and unpredictable set of data
10 309. The set of data 309 thus can function as a robust keyword seed.

11
12 Figure 5 is a flowchart 500 of a method for multimedia encryption. The
13 method begins in step 502 where the transducer 102 receives a media signal
14 which may include a noise signal amplitude. In step 504, the A/D converter
15 106 quantizes the media signal with a quantization step size smaller than the
16 noise signal amplitude. The data compression module 302 compress the
17 media signal into data frames having data frame boundaries, where the data
18 frames may have similar or varying lengths, include compression transform
19 coefficients, and/or include predictive data frames in step 506. Next, in step
20 508, the data acquisition module 308 selects a set of data from the compressed
21 media signal, such that the data selected may include one frame of data, data
22 which crosses over several data frame boundaries, compression transform
23 coefficients, and/or predictive data frames. In step 510, the message digest

1 generator 310 hashes the set of data into a keyword. After step 510, the
2 method is complete.

3

4 While the present invention has been described with reference to a
5 preferred embodiment, those skilled in the art will recognize that various
6 modifications may be made. Variations upon and modifications to the
7 preferred embodiment are provided by the present invention, which is
8 limited only by the following claims.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2

WHAT IS CLAIMED IS:

- 1 1. A system for multimedia encryption comprising:
 - 2 a media signal;
 - 3 a data compression module coupled to receive and compress the media
 - 4 signal into a compressed data stream;
 - 5 a data acquisition module coupled to receive and select a set of data
 - 6 from the compressed data stream; and
 - 7 a hashing module coupled to receive and hash the set of data into a
 - 8 keyword.
- 1 2. The system of claim 1 wherein the set of data is one frame of data
- 2 within the compressed data stream.
- 1 3. The system of claim 1 wherein the set of data crosses over several
- 2 frame boundaries within the compressed data stream.
- 1 4. The system of claim 1 wherein:
 - 2 the compressed data stream includes compression transform
 - 3 coefficients; and
 - 4 the set of data includes a set of compression transform coefficients.
- 1 5. The system of claim 1 wherein:
 - 2 the compressed data stream includes data frames of varying length; and

3 the set of data includes a set of data frames.

1 6. The system of claim 1 wherein:

2 the compressed data stream includes predictive data frames; and

3 the set of data includes a predictive data frame.

1 7. The system of claim 1:

2 wherein the media signal includes a noise signal amplitude;

3 further comprising,

4 an analog to digital converter, having a quantization step size

5 smaller than the noise signal amplitude, coupled to receive and

6 quantize the media signal; and

7 wherein the data compression module compresses the quantized

8 media signal into a compressed data stream.

1 8. The system of claim 1 wherein the data compression module

2 compresses the media signal into one from a group consisting of: MJPEG,

3 MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats.

1 9. The system of claim 1 further comprising:

2 a pseudo-random number generator coupled to receive and process the

3 keyword in to a set of keywords.

1 10. A method for multimedia encryption, comprising the steps of:
2 compressing a media signal;
3 selecting a set of data from the compressed media signal; and
4 hashing the set of data into a keyword.

1 11. The method of claim 10 wherein:
2 the compressed media signal includes data frames; and
3 the selecting step includes the step of selecting one frame of data.

1 12. The method of claim 10 wherein:
2 the compressed media signal includes data frames and data frame
3 boundaries; and
4 the selecting step includes the step of selecting a set of data which
5 crosses over several data frame boundaries.

1 13. The method of claim 10 wherein:
2 the compressed media signal includes compression transform
3 coefficients; and
4 the selecting step includes the step of selecting a set of compression
5 transform coefficients.

1 14. The method of claim 10 wherein:

2 the compressed media signal includes data frames of varying length;
3 and
4 the selecting step includes the step of selecting a set of data frames.

1 15. The method of claim 10 wherein:
2 the compressed media signal includes predictive data frames; and
3 the selecting step includes the step of selecting a predictive data frame.

1 16. The method of claim 10:
2 wherein the media signal includes a noise signal amplitude;
3 further comprising the step of quantizing the media signal with a
4 quantization step size smaller than the noise signal amplitude; and
5 wherein the compressing step includes the step of compressing the
6 quantized media signal.

1 17. A system for multimedia encryption, comprising:
2 means for compressing a media signal;
3 means for selecting a set of data from the compressed media signal; and
4 means for hashing the set of data into a keyword.

1 18. The system of claim 17 wherein:
2 the compressed media signal includes data frames; and
3 the means for selecting includes means for selecting one frame of data.

1 19. The system of claim 17 wherein:
2 the compressed media signal includes data frames and data frame
3 boundaries; and
4 the means for selecting includes means for selecting a set of data which
5 crosses over several data frame boundaries.

1 20. The system of claim 17 wherein:
2 the compressed media signal includes compression transform
3 coefficients; and
4 the means for selecting includes means for selecting a set of
5 compression transform coefficients.

1 21. The system of claim 17 wherein:
2 the compressed media signal includes data frames of varying length;
3 and
4 the means for selecting includes means for selecting a set of data
5 frames.

1 22. The system of claim 17 wherein:
2 the compressed media signal includes predictive data frames; and
3 the means for selecting includes means for selecting a predictive data
4 frame.

1 23. The system of claim 17:
2 wherein the media signal includes a noise signal amplitude;
3 further comprising means for quantizing the media signal with a
4 quantization step size smaller than the noise signal amplitude; and
5 wherein the means for compressing includes means for compressing
6 the quantized media signal.

1 24. A computer-useable medium embodying computer program code for
2 multimedia encryption by executing the steps of:
3 compressing a media signal;
4 selecting a set of data from the compressed media signal; and
5 hashing the set of data into a keyword.

1 25. The computer-useable medium of claim 24 wherein:
2 the compressed media signal includes data frames; and
3 the selecting step includes the step of selecting one frame of data.

1 26. The computer-useable medium of claim 24 wherein:
2 the compressed media signal includes data frames and data frame
3 boundaries; and
4 the selecting step includes the step of selecting a set of data which
5 crosses over several data frame boundaries.

1 27. The computer-useable medium of claim 24 wherein:
2 the compressed media signal includes compression transform
3 coefficients; and
4 the selecting step includes the step of selecting a set of compression
5 transform coefficients.

1 28. The computer-useable medium of claim 24 wherein:
2 the compressed media signal includes data frames of varying length;
3 and
4 the selecting step includes the step of selecting a set of data frames.

1 29. The computer-useable medium of claim 24 wherein:
2 the compressed media signal includes predictive data frames; and
3 the selecting step includes the step of selecting a predictive data frame.

1 30. The computer-useable medium of claim 24:
2 wherein the media signal includes a noise signal amplitude;
3 further comprising the step of quantizing the media signal with a
4 quantization step size smaller than the noise signal amplitude; and
5 wherein the compressing step includes the step of compressing the
6 quantized media signal.

1 SYSTEM AND METHOD FOR MULTIMEDIA ENCRYPTION

2 ABSTRACT OF THE DISCLOSURE

3 A system and method is disclosed for multimedia encryption. Within
4 the system of the present invention, a data compression module receives and
5 compresses a media signal into a compressed data stream. A data acquisition
6 module receives and selects a set of data from the compressed data stream.
7 And, a hashing module receives and hashes the set of data into a keyword.
8 The method of the present invention includes the steps of compressing a
9 media signal into a compressed data stream; selecting a set of data from the
10 compressed data stream; and hashing the set of data into a keyword.

100 102 106 110

100 ↗

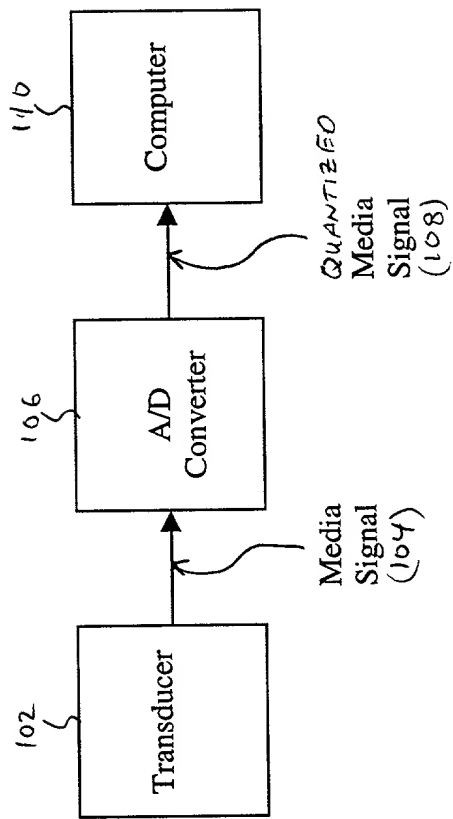


FIG. 1

260 ↗

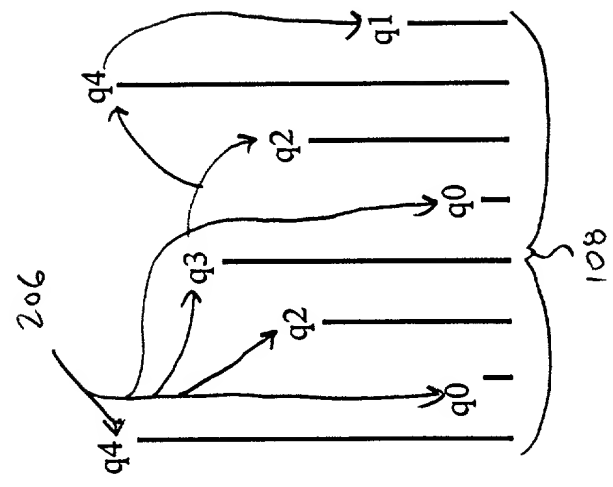
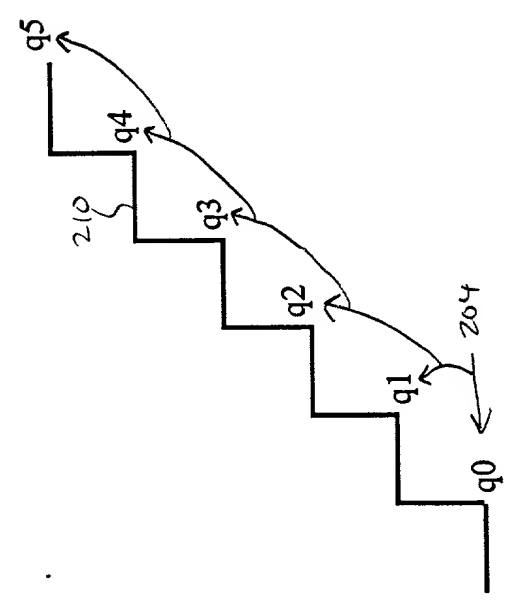
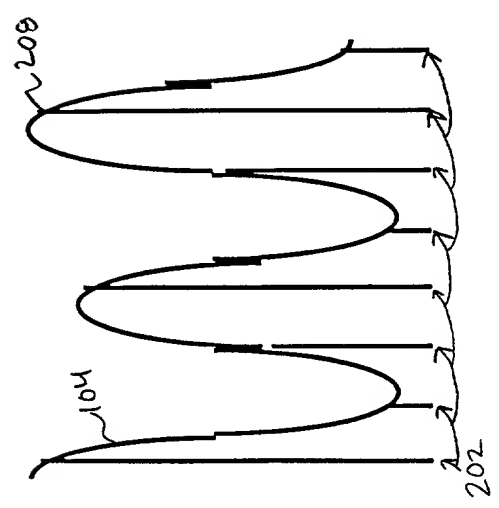


FIG. 2

300 →

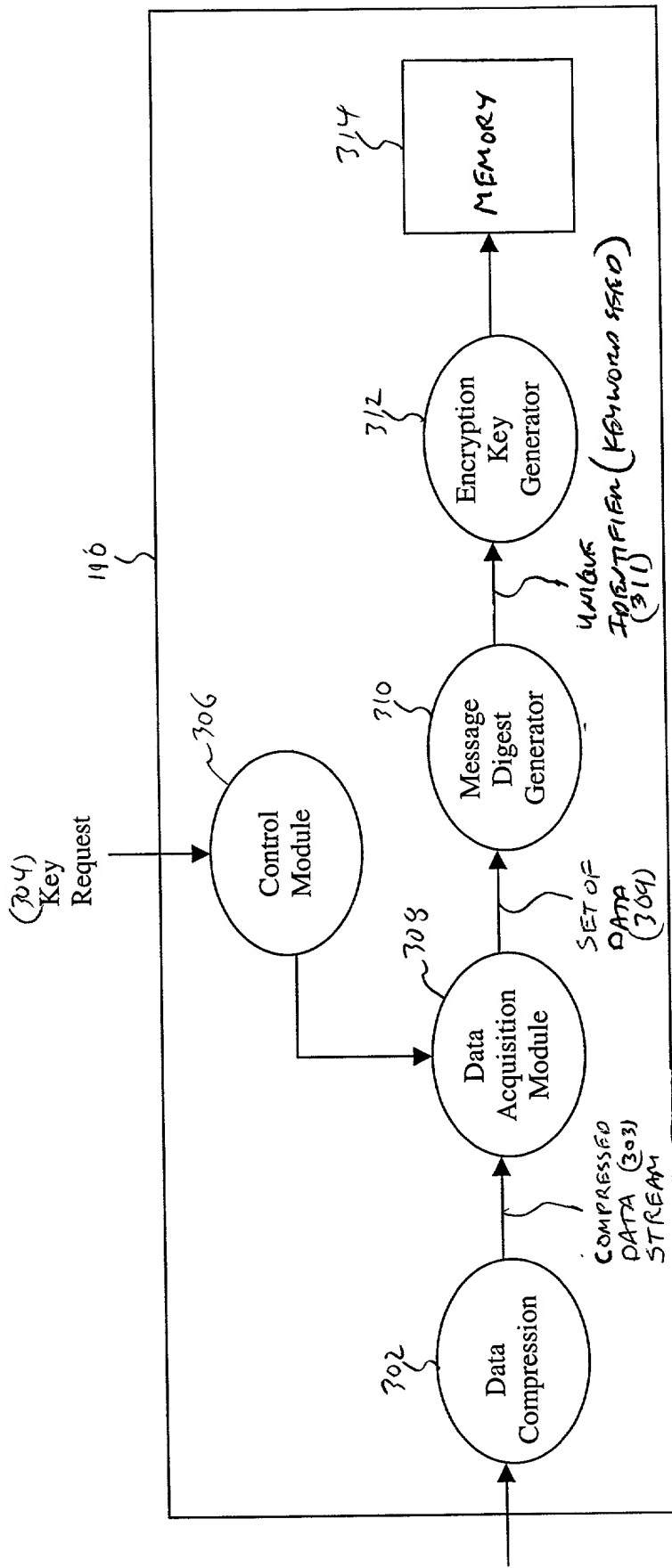


FIG. 3

400 →

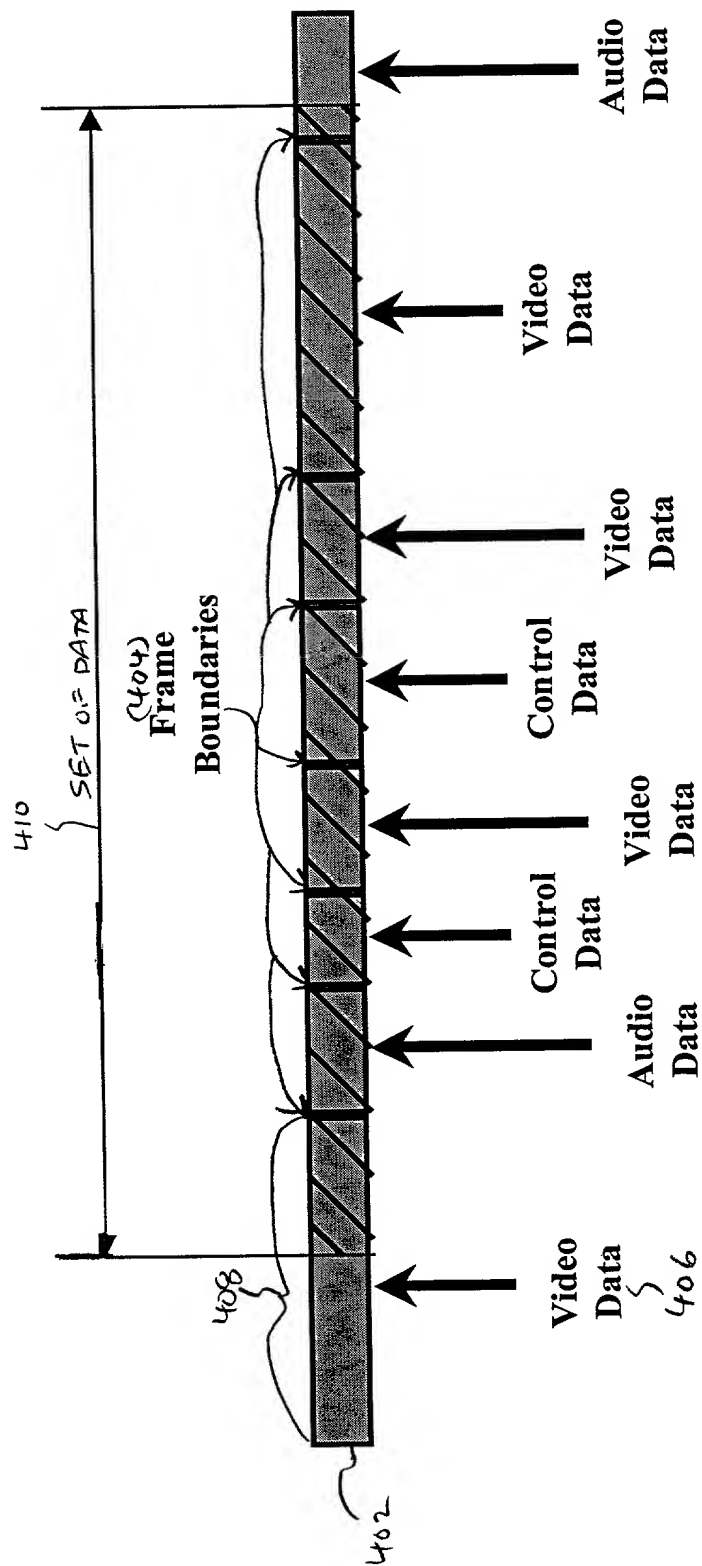


FIG. 4

5/5

500



Start
Encryption
Routine

Acquire a media signal which may include a noise signal amplitude

502

Quantize the media signal with a quantization step size smaller than the noise
signal amplitude

504

Compress the media signal into data frames having data frame boundaries, where
the data frames may have similar or varying lengths, include compression
transform coefficients, and/or include predictive data frames

506

Select a set of data from the compressed media signal, such that the data selected
may include one frame of data, data which crosses over several data frame
boundaries, compression transform coefficients, and/or predictive data frames

508

Hash the set of data into a keyword

510

End

FIG. 5

COMBINED DECLARATION AND POWER OF ATTORNEY

- ☒ Declaration submitted
with Initial Filing
- ☐ Declaration submitted
after Initial Filing (surcharge
(37 CFR 1.16(e)) required)

Attorney Docket: IL-10360
Applicant: Douglas R. Coffland
Serial No.:
Filing Date:

As a below named inventor(s), I (we) hereby declare that:

My (Our) residence, post office address and citizenship(s) are as stated below next to my (our) name(s).

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: _____

System and Method for Multimedia Encryption

the specification of which (check one)

X is attached hereto _____ was filed on _____ as United States Application Number
or PCT International Application Number _____

and was amended on _____ (if applicable).

I (We) hereby state that I (we) have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I (We) acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I (We) hereby claim foreign priority benefits under 35, U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

(Application Number) (Country) (Foreign Filing Date)



(Application Number) (Country) (Foreign Filing Date)



I (We) hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below:

Application Serial No. Filing Date

Application Serial No. Filing Date


I (We) hereby claim the benefit under 35 U.S.C. 120 of any United States applications(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

Application Serial No.	Filing Date	Status
------------------------	-------------	--------

POWER OF ATTORNEY: As the named inventor(s), I (we) hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Names	Registration No.
Lloyd E. Dakin, Jr.	38,423
John P. Wooldridge	38,725
<u>Direct Correspondence To:</u> Lloyd E. Dakin, Jr. Assistant Laboratory Counsel Lawrence Livermore National Laboratory P.O. Box 808 - L-703 Livermore, California 94551	<u>Direct Telephone Calls To:</u> (Name and Telephone Numbers) Lloyd E. Dakin, Jr. (925) 423-8554

I (We) hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Douglas R. Coffland	
Full Name of Inventor	Signature
Livermore, California	9/10/99
Residence (City, State or Foreign Country)	Date
5674 Wisteria Way, Livermore, CA 94550	USA
Postal Address (Street, City, State, Zip Code)	Citizenship
XX	
Full Name of Inventor	Signature
Residence (City, State or Foreign Country)	Date
Postal Address (Street, City, State, Zip Code)	Citizenship
XX	